

# UNITED STATES DISTRICT COURT

## EASTERN DISTRICT OF WISCONSIN

CLERK'S OFFICE

A TRUE COPY

Aug 28, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

In the Matter of the Seizure of  
(Address or brief description of property or premises to be seized)

UP TO 489,269.52 TETHER (USDT) CRYPTOCURRENCY ON  
DEPOSIT IN THE KRAKEN USER ID AA27 N84G RDV7 WHDA  
HELD IN THE NAME OF OSL SG PTE LTD

Case Number: 23 MJ 160

### APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, Nicholas Schlereth, being duly sworn depose and say:

I am a Special Agent with the United States Secret Service and have reason to believe that in the Northern District of California there is now certain property, namely, up to 489,269.52 Tether (USDT) cryptocurrency on deposit in the Kraken User ID AA27 N84G RDV7 WHDA held in the name of OSL SG PTE LTD, that is (1) civilly forfeitable under 18 U.S.C. §§ 981(a)(1)(C) and 984, including cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), and criminally forfeitable under 18 U.S.C. § 981(a)(1)(C) in conjunction with 28 U.S.C. § 2461(c), as funds that consist of, or are traceable to, proceeds of wire fraud committed in violation of 18 U.S.C. § 1343; and (2) civilly forfeitable under 18 U.S.C. §§ 981(a)(1)(A) and 984, and criminally forfeitable under 18 U.S.C. § 982(a)(1), as funds involved in, or traceable to funds involved in, money laundering offenses committed in violation of 18 U.S.C. §§ 1956 and 1957, and is therefore also subject to seizure for purposes of civil forfeiture under 18 U.S.C. § 981(b), and for purposes of criminal forfeiture under 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(f).

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone and email.

8/28/2023 at 12:38 PM  
Date and time issued

William E. Duffin, U.S. Magistrate Judge  
Name & Title of Judicial Officer

Nicholas Schlereth

Signature of Affiant  
Nicholas Schlereth, USSS

at Milwaukee, Wisconsin  
City and State

William E. Duffin  
Signature of Judicial Officer

## **AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT**

I, Nicholas Schlereth, have been duly sworn on oath, state as follows:

### **Affiant's Background**

1. I am a Special Agent with the United States Secret Service ("USSS"). I have been so employed since 2021. I am a member of the USSS's Cyber Fraud Task Force. As part of my duties as a USSS Special Agent, I investigate violations related to mail, wire and bank fraud, as well as identity theft. I have received training in conducting criminal investigations, including physical and electronic surveillance, interviewing witnesses, and executing search and seizure warrants.

2. I have received over 1,200 hours of training in network intrusion response, money laundering and asset forfeiture, and cryptocurrency investigations offered through the Federal Law Enforcement Training Center and the United States Secret Service. I have received advanced training in for cryptocurrency related investigations and am the subject matter expert (SME) for cryptocurrency in the Chicago Field Office. I perform investigations involving both domestic and international subjects that utilize electronic devices and the financial infrastructure in the furtherance of criminal violations.

### **Property Sought to be Seized**

3. I submit this affidavit in support of an application for a warrant to seize up to 489,269.52 Tether (USDT) cryptocurrency in the **Kraken User ID AA27 N84G RDV7 WHDA** held in the name of OSL SG PTE LTD.

4. For the reasons set forth below, I submit that up to 489,269.52 Tether (USDT) cryptocurrency held in the **Kraken User ID AA27 N84G RDV7 WHDA** are:

- a. Funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343, and therefore are subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(C) and 984, including cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), and subject to criminal forfeiture under 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c);
- b. Funds involved in, or traceable to funds involved in, money laundering offenses, committed in violation of 18 U.S.C. §§ 1956 and 1957, and therefore are subject to civil forfeiture under 18 U.S.C. §§ 981 (a)(1)(A) and 984, and subject to criminal forfeiture under 18 U.S.C. § 982(a)(1); and
- c. Subject to seizure via a civil seizure warrant under 18 U.S.C. § 981(b)(2) and via a criminal seizure warrant under 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(f).

### **Summary of Scheme to Defraud**

5. There is probable cause to believe that up to \$500,000 in proceeds of a wire fraud/romance scheme, also known as “pig butchering” (see definition below) were involved in material misrepresentations and the use of cryptocurrency transactions that are a combination of domestic and international wires in connection with a “pig-butcher” fraud scam have been deposited, and comingled with other funds, in **Kraken User ID AA27 N84G RDV7 WHDA**.

6. As part of the “pig butchering” fraud scam, an unknown suspect caused/directed/advised the victim, located within the Eastern District of Wisconsin, to transfer approximately \$432,900 in U.S. currency to a domain name purporting to be the New York Stock Exchange utilizing cryptocurrency.

### **Cryptocurrency Definitions**

7. Kraken: A secure online cryptocurrency exchange where an individual can buy, sell, transfer and store cryptocurrency whose registration shows that Kraken is located in Malta. According to the Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money service businesses. Such exchanges and exchangers are required to register with FinCEN and have proper state licenses, if required under applicable state law.

8. Cryptocurrency: A type of virtual currency in a decentralized, peer-to-peer network medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services, or exchanged for fiat currency or other cryptocurrencies. Individuals can obtain cryptocurrency through exchanges and other intermediaries, person-to-person transfers, the sale of goods or services, or mining. There are thousands of cryptocurrencies including Bitcoin (“BTC”) and Tether (“USDT”).

9. Cryptocurrency Exchange: A business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies. Exchanges may accept credit card payments, wire transfers or other forms of payments in exchange for digital currencies or cryptocurrencies.

10. Fiat Currency: Coin and paper money of a country that has legal tender.

11. Blockchain: Most cryptocurrencies have a “Blockchain,” which is a decentralized, typically public, transaction ledger containing an immutable and historical record of every transaction involving the cryptocurrency. Some cryptocurrencies operate on Blockchains that are not transparent or have built-in, protocols designed to conceal transactional information in the furtherance of money laundering making it difficult to trace or attribute transactions. Though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities are not recorded on these public ledgers.

12. Blockchain Analysis: The process of inspecting, identifying, clustering, modeling and visually representing data on a cryptographic, distributed-ledger known as a Blockchain. Data

in most Blockchains is public, meaning anyone can view the contents. The goal of Blockchain analysis is discovering useful information about the different actors transacting in cryptocurrency by using open source and/or subscription analytical tools, such as “Chainalysis” to determine what transactions were conducted by that individual or entity. Cryptocurrency transactions are sometimes referred to a “pseudonymous,” meaning that they are partially anonymous.

13. Transaction Hash: A unique string of characters that is given to every transaction that is verified and added to the Blockchain.

14. Wallet: A wallet is a software program that interfaces with the Blockchain and generates and stores public and private keys used to send and receive cryptocurrencies. A wallet can have one or more cryptocurrency address(es) that are controlled by the same individual or entity.

15. Bitcoin/Cryptocurrency Address: A public address, which is represented as a case-sensitive string of letters and numbers, is akin to a bank account number, and a private key is a cryptographic equivalent of a Personal Identification Number (PIN) or password.

16. Pig Butchering Scheme/Scam: A pig butchering scheme contains is rooted in an investment/securities fraud. It can have elements of a romance scam, but the goal is to bleed out as much money from a victim by leading them to invest in various cryptocurrency domains. The suspects offer high returns for their investments and direct the victim to custom created websites that make it appear as if they are investing by showing the victim gains in their investment. When the victim requests to withdraw fiat currency from the investment portal, they are told they have to pay a tax. Even after paying the tax, the funds are not released, and the suspects usually come up with another fee or aspect to get more funds from the victim. The same process continues until the victim states they are done, which is usually followed by the suspects saying they will invest their own funds to help the suspect continue the scheme.

17. Although cryptocurrencies such as Bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple address and/or wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track transactions.

### **Statement of Probable Cause** **Brookfield, WI Fraud Case**

18. On or about June 14, 2023, the United States Secret Service, Milwaukee Resident Office was contacted by an individual having the initials K.Z., who resides at 1XXX Club Cir., Apt. XXX, City of Brookfield, Wisconsin, K.Z reported that he was a victim of fraud in the amount of approximately \$433,000.

19. K.Z. stated that in late July or early August 2022, he was contacted by a woman named “Diane Meyer” on Facebook. K.Z. stated that he did not know Meyer prior to her contacting him on Facebook. After initially developing what K.Z. stated as a “friendship,” Meyer broached

the idea of trading Bitcoin, claiming it would be a profitable experience. K.Z. resisted the investment opportunity, which led to Meyer not talking to him for a month.

20. In November 2022, Meyer re-engaged K.Z. regarding Bitcoin investments K.Z. stated he gave in and proceeded with the investment opportunity. After agreeing to participate, Meyer directed K.Z. to create accounts at the cryptocurrency exchanges Coinbase.com and Crypto.com. Based on my training and experience, and the investigation to date, I am aware that Cross River Bank and Metropolitan Commercial Bank are the commercial banks for Coinbase.com and Crypto.com, respectively. The banks operate “For Benefit Of” accounts for their clients, enabling clients to wire funds directly to the exchange for the purchase of cryptocurrency.

21. Between November 7, 2022 and June 2, 2023, K.Z. sent three (3) wires to Cross River Bank (Coinbase.com) and nineteen (19) wires to Metropolitan Commercial Bank (Crypto.com) from his bank account at Landmark Credit Union. The funds sent to Cross River Bank were sent with the beneficiary code (326997647689) and the funds sent to Metropolitan Commercial Bank were sent with the beneficiary code (364380200290). The beneficiary codes are assigned to the specific account holder at the bank, for the inbound funds from a wire to be allocated to the proper account holder within the exchange. Table 1 includes a breakdown of K.Z.’s wire transfers to Cross River Bank and Metropolitan Commercial Bank.

Table 1. K.Z Wire Transfers to Cross River Bank & Metropolitan Commercial Bank:

<b>Date</b>	<b>Amount</b>	<b>Bank</b>
11/07/22	\$5,000	Metropolitan Commercial Bank
11/28/22	\$19,000	Metropolitan Commercial Bank
12/02/22	\$30,000	Cross River Bank
12/22/22	\$45,000	Cross River Bank
12/23/22	\$42,000	Metropolitan Commercial Bank
12/30/22	\$10,000	Metropolitan Commercial Bank
01/26/23	\$100,000	Cross River Bank
01/30/23	\$250,000	Metropolitan Commercial Bank <ul style="list-style-type: none"> <li>• Traced 130,000 USDT from this transaction</li> </ul>
02/08/23	\$30,000	Metropolitan Commercial Bank
02/16/23	\$1,000	Metropolitan Commercial Bank
02/23/23	\$15,000	Metropolitan Commercial Bank
03/02/23	\$15,000	Metropolitan Commercial Bank
03/07/23	\$15,000	Metropolitan Commercial Bank
03/09/23	\$15,000	Metropolitan Commercial Bank
03/13/23	\$20,000	Metropolitan Commercial Bank
03/20/23	\$8,000	Metropolitan Commercial Bank
03/21/23	\$2,000	Metropolitan Commercial Bank
04/10/23	\$1,000	Metropolitan Commercial Bank
05/20/23	\$400	Metropolitan Commercial Bank
05/26/23	\$500	Metropolitan Commercial Bank
06/01/23	\$5,000	Metropolitan Commercial Bank
06/02/23	\$5,000	Metropolitan Commercial Bank

<b>TOTAL</b>	<b>\$633,900.00</b>	<b>Wire Transfers to Crypto Exchanges</b>
<b>Minus</b>	<b>\$144,630.48</b>	<b>Withdrawn to K.Z.'s Bank Accounts</b>
<b>TOTAL</b>	<b>\$489,269.52</b>	<b>Total Fraud Loss Experienced by K.Z.</b>

22. After depositing funds into Coinbase.com and Crypto.com, Meyer directed K.Z. to purchase Tether (USDT) cryptocurrency. K.Z. stated that he believed that he was investing through the New York Stock Exchange (NYSE) based on guidance from Meyer. After he tried to send approximately 90,000 USDT using the Coinbase account, K.Z. stated Coinbase.com denied the transactions from going through due to presumed fraud associated with the account activity. Based on records provided by K.Z., K.Z. withdrew his funds (approximately \$144,149.48) from Coinbase and only utilized the Crypto.com account. K.Z.'s Crypto.com records indicate that he withdrew (approximately \$481.00) from his account on April 16, 2023, all other funds deposited to the Crypto.com (Metropolitan Commercial Bank) were sent out as USDT or Bitcoin.

23. The domain that K.Z. invested through and which purported to be the NYSE was [www.nysefree.com/h5/#/](http://www.nysefree.com/h5/#/). The domain was reported in numerous other incidents inside the Consumer Sentinel database as being a fraudulent cryptocurrency investment portal. All reports describe a similar scheme where once profits were shown in the account and funds were attempted to be withdrawn, the victims were told they would have to prepay taxes on the investment before funds could be released.

24. The domain [www.nysefree.com/h5/#/](http://www.nysefree.com/h5/#/) was searched in the FBI's IC3 database. Numerous results were returned stating the domain was a fraudulent cryptocurrency investment portal. The reports outlined similar instances where victims were contacted by a woman on Facebook who discussed cryptocurrency investments. The women recommended investing through the provided domain. Once the victim sought to withdraw funds, they were told they had to prepay taxes on the investment or funds would not be released.

25. A Domain Name Server (DNS) inquiry was conducted on the domain [www.nysefree.com/h5/#/](http://www.nysefree.com/h5/#/). The domain was registered on November 5, 2022 by the registrar company, maff.com. The domain corresponds to IP address 18.230.170.72, and is being hosted on a server run by Amazon Digital Services in Brazil.

26. After seeing success with his investments, K.Z. wanted to withdraw his profits from the investments. K.Z. was instructed that he would have to prepay his taxes for the investment. He was told that he would have to pay approximately 180,000 USDT as his taxes. K.Z. did not have the funds to submit the payment. He periodically would consult the NYSE customer support feature to inquire about his account to get updates on if his funds were still available. The subsequent paragraphs outline communications between K.Z. and the NYSE customer support line.

27. On March 10, 2023, K.Z. submitted an inquiry to the purported NYSE customer support line where he was told "once your payment is complete, the bank escrow account will automatically release the funds. To avoid affecting your credit and paying more in late fees, please complete your tax payment within the specified time frame."

28. On May 21, 2023, The purported NYSE customer support stated that K.Z. would have to pay his personal income tax of 186,867.903872 USDT. K.Z. would have to pay the tax in cryptocurrency. After paying the tax, he would be able to withdraw his proceeds as cash. At the same point, it was confirmed to him that he had 912,427.0796 USDT deposited into a third-party bank supervision account, as a holding spot until his tax payment was processed. K.Z. stated he did not have the funds and would not be able to prepay his taxes on the investment gains.

29. On July 17, 2023, K.Z. received a call from Vince Woods, who represented to be the Head of Finance for NYSE (872-205-9525) and who claimed that he wanted to help K.Z. get his funds out of the purported NYSE. K.Z. stated that Woods offered to cut his tax payment in half to facilitate the return of K.Z.'s presumed profits in the NYSE platform. A database search was conducted on the phone number 872-205-9525 and it returned to Bandwidth.com as a Voice Over Internet Protocol (VOIP) phone number. Based on my training and experience, and the investigation to date, case agents believe that the individual who purported to be the NYSE Head of Finance was attempting to get additional money from K.Z. in exchange for falsely promising to return the funds that K.Z. believed he invested in the NYSE.

### **Brookfield, WI Cryptocurrency Tracing**

30. The tracing of cryptocurrency in this case was done using the accounting technique of Last In, First Out (LIFO). The methodology was applied starting with the initial deposit of the victim's cryptocurrency into the initial address. Since the funds were derived in a fraudulent manner, the assumption was made that the victim's cryptocurrency upon entry to the initial address made all other cryptocurrency in that address tainted. LIFO was applied to the tracing of funds in this case.

31. Blockchain analytics tools, like Chainalysis and/or TRM, were utilized to conduct the tracing in this case. All tracing was validated against the blockchain available in distributed public registers available via the internet.

32. On February 1, 2023, K.Z. sent 139,322 Tether (USDT) to the deposit address (0x6e051Bd993561D825d5c61A1B120Fd435264**6f5d**). K.Z. stated the (0x6e051Bd993561D825d5c61A1B120Fd435264**6f5d**) address belonged to NYSE and was directed to him by Meyer.

33. The next day, February 2, 2023, the 139,322 Tether (USDT) deposited by K.Z. on February 1, 2023 to (0x6e051Bd993561D825d5c61A1B120Fd435264**6f5d**) was comingled with other USDT in seven (7) other addresses before landing at the address (0x61B7Fb34a12B7018cD57dfDFa091710f18d32**cBa**). The address was a deposit address with Binance cryptocurrency exchange.

34. On June 13, 2023, law enforcement sent an information request to Binance to seek account details and know your customer (KYC) documentation for the address (0x61B7Fb34a12B7018cD57dfDFa091710f18d32**cBa**).

35. On June 14, 2023, Binance responded with account details and KYC documentation for the account. The Binance records confirm the deposit of 137,752 USDT into account #: 162574816 on February 2, 2023 at 06:28 UTC. The account belonged to ANNOP SOPHITRUNGRUEAR, a Thailand citizen, confirmed through the presence of a Thai National ID Card attached to the account. Applying LIFO to the account, 60,011 USDT was withdrawn from the Binance account the same day as the 137,752 USDT deposit, and sent to Tether (as a TRC20 token) to the address (TETbBCB3SZrVKmqwrXv21CJf6mq2Gg**3Rz**).

36. The Tether sent on February 2, 2023 from the Binance Account belong to SOPHITRUNGRUEAR, was sent across 22 other addresses before landing in the address (TWbkrDKpYG14ZhvoP5GjHfJyFyg9pb**Stjg**). The address is a deposit address for an account at Kraken cryptocurrency exchange.

### **Identifying the Kraken account of User ID AA27 N84G RDV7 WHDA**

37. On June 16, 2023, law enforcement requested information from for the account associated to the address (TWbkrDKpYG14ZhvoP5GjHfJyFyg9pb**Stjg**) and transaction hash (397cb2bad8054f449c40c48f9a9dda130fb7b6d6aee8c671ac4678827fe2f06e). Kraken confirmed that this address is associated with **Kraken User ID AA27 N84G RDV7 WHDA**. Kraken provided the identifiers that are associated with **Kraken User ID AA27 N84G RDV7 WHDA**. According to Kraken records, Kraken User ID AA27 N84G RDV7 WHDA is in the name of OSL SG PTE LTD, whose account was registered on January 12, 2021 utilizing corporate documents for OSL SG PTE LTD, and a passport for a United Kingdom citizen, Suzanne JENSEN.

38. OSL SG PTE LTD is registered with the User ID (detectorforumwords) and the email address (sgtrader@osl.com). OSL SG PTE LTD is listed at the address, 1 Joo Chiat Road, #05-1005, Joo Chiat Complex, North East Community Development Region, 420001, Singapore. The Employee Identification Number provided to Kraken by OSL SG PTE LTD was 201836009D.

39. Kraken's records show the deposit 6,417,000 USDT into the account belonging to the **Kraken User ID AA27 N84G RDV7 WHDA**.

### **Applicable Asset Forfeiture Provisions**

40. Under 18 U.S.C. § 984, a court may order the forfeiture of funds in a bank account into which monies subject to forfeiture have been deposited, without the need to trace the funds currently in the account to the specific deposits that are subject to forfeiture, up to the amount of the funds subject to forfeiture that have been deposited into the account within the past one-year period.

41. Section 984 (a) provides in part:

(1) In any forfeiture action in rem in which the subject property is cash [or] funds deposited in an account in a financial institution



(A) it shall not be necessary for the Government to identify the specific property involved in the offense that is the basis for the forfeiture; and

(B) it shall not be a defense that the property involved in such an offense has been removed and replaced by identical property.

(2) Except as provided in subsection (c), any identical property found in the same place or account as the property involved in the offense that is the basis for the forfeiture shall be subject to forfeiture under this section.

42. 18 U.S.C. § 984(b) provides: “No action pursuant to this section to forfeit property not traceable directly to the offense that is the basis for the forfeiture may be commenced more than 1 year from the date of the offense.”

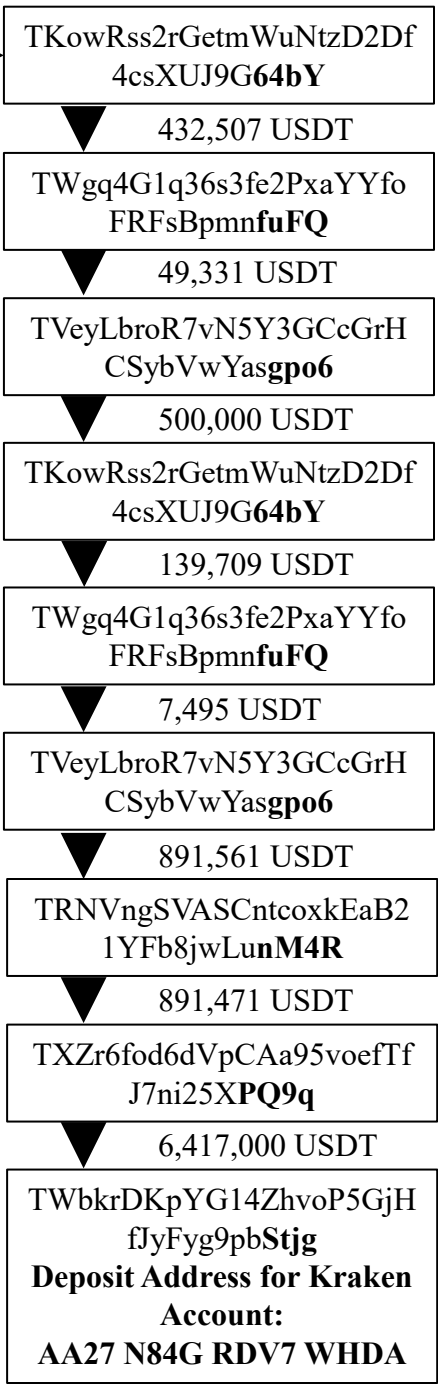
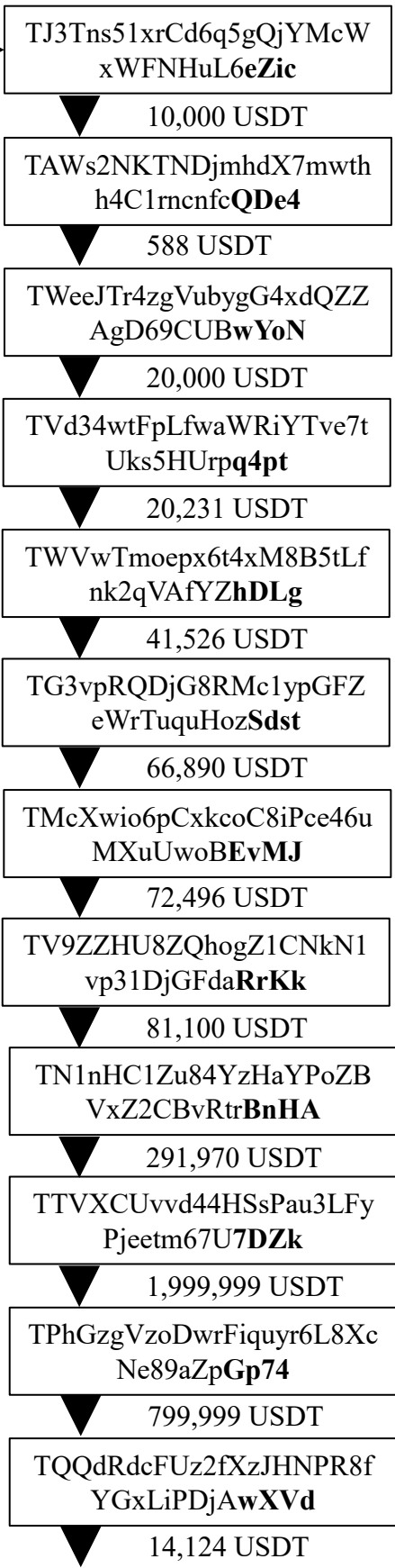
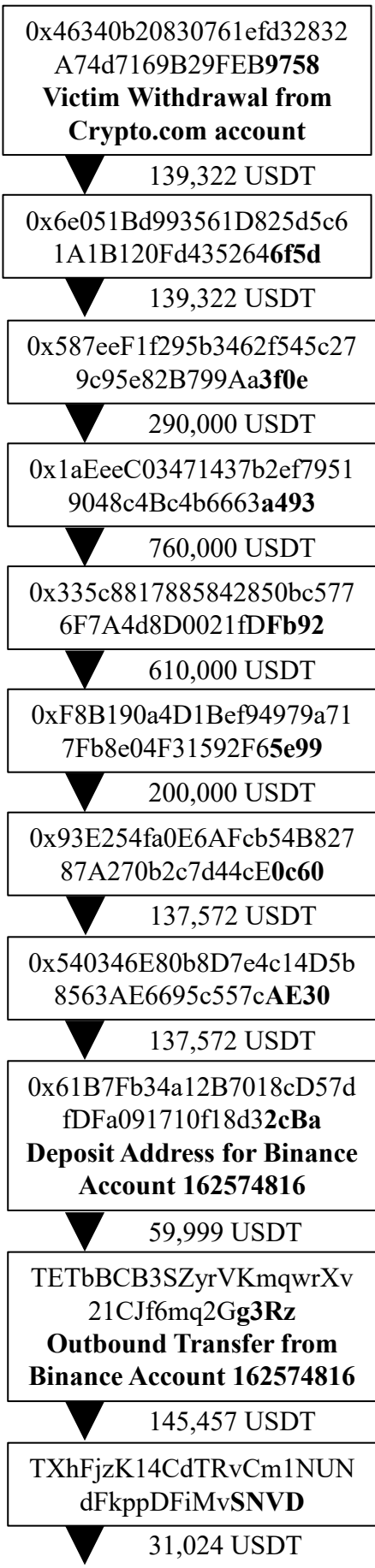
43. Thus, under Section 984, a court may order the civil forfeiture of monies found in a bank account into which deposits of criminal proceeds subject to forfeiture had been made, up to the amount of the forfeitable deposits that have been made into the account within the prior one-year period, without the need for tracing the funds to be forfeited to any of the specific forfeitable deposits.

44. I submit that a restraining order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the funds for forfeiture because I have been advised of cases in which, even after restraining order or similar process has been issued to financial institution, the funds sought to be restrained were not effectively restrained by the financial institution. In my judgment, a seizure warrant would be the most effective way to assure the availability of the money sought to be seized for forfeiture.

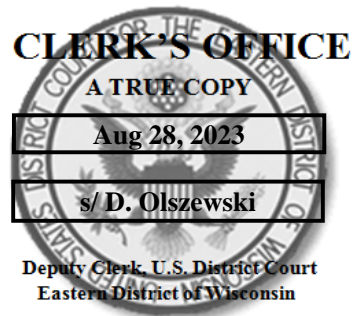
### **Conclusion**

45. Based on the facts and circumstances set forth in this affidavit, I submit that there exists probable cause to believe that up to 489,269.52 Tether (USDT) cryptocurrency in the **Kraken User ID AA27 N84G RDV7 WHDA** held in the name of OSL SG PTE LTD:

- a. Funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343, and therefore are subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(C) and 984, including cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), and subject to criminal forfeiture under 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c);
- b. Funds involved in, or traceable to funds involved in, money laundering offenses, committed in violation of 18 U.S.C. §§ 1956 and 1957, and therefore are subject to civil forfeiture under 18 U.S.C. §§ 981 (a)(1)(A) and 984, and subject to criminal forfeiture under 18 U.S.C. § 982(a)(1); and
- c. Subject to seizure via a civil seizure warrant under 18 U.S.C. § 981(b)(2) and via a criminal seizure warrant under 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(f).



UNITED STATES DISTRICT COURT  
for the  
EASTERN DISTRICT OF WISCONSIN



In the Matter of the Seizure of  
(Address or brief description of property or premises to be seized)

UP TO 489,269.52 TETHER (USDT) CRYPTOCURRENCY ON Case Number: 23 MJ 160  
DEPOSIT IN THE KRAKEN USER ID AA27 N84G RDV7 WHDA  
HELD IN THE NAME OF OSL SG PTE LTD

**WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE**

**TO: NICHOLAS SCHLERETH, a Special Agent with the United States Secret Service, and  
any Authorized Officer of the United States.**

An application by a federal law enforcement officer or an attorney for the government requests that certain property be seized as being subject to forfeiture to the United States of America. The property is described as follows:

Up to 489,269.52 Tether (USDT) cryptocurrency on deposit in the Kraken User ID AA27 N84G RDV7 WHDA held in the name of OSL SG PTE LTD

I find that the affidavit and any recorded testimony establish probable cause to seize the property.

**YOU ARE HEREBY COMMANDED** to search on or before September 11, 2023  
(not to exceed 14 days)

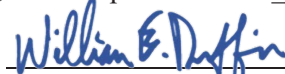
☐ in the daytime – 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night, as I find  
reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge William E. Duffin.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. §2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person, who, or whose property, will be searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days. (not to exceed 30)  
☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued 8/28, 2023; 12:38 p.m.

  
Judge's signature

City and state: Milwaukee, Wisconsin

THE HONORABLE WILLIAM E. DUFFIN  
United States Magistrate Judge  
Name & Title of Judicial Officer

## Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

*Executing officer's signature*

---

Printed name and title